Chapter 3

Skew Cyclic Codes over $\mathbb{F}_q[u_1, u_2, \ldots, u_r]/\langle u_i^3 - u_i, u_iu_j - u_ju_i\rangle_{i,j=1}^{r}$

In this chapter, we study skew cyclic codes over a finite non-chain ring $\mathbb{F}_q[u_1, u_2, \ldots, u_r]/\langle u_i^3 - u_i, u_iu_j - u_ju_i\rangle$ denoted as $\mathcal{R}$. Initially, we examine some key properties of $\mathcal{R}$. Further, we define a Gray map on $\mathcal{R}$ and establish its distance-preserving and orthogonality-preserving properties. Then, we discuss the structural properties of linear codes over $\mathcal{R}$ and provide an explicit form of the generator matrix for the Gray image of a linear code over $\mathcal{R}$.

In Section 3.4, we delve into essential properties of automorphisms of $\mathcal{R}$, followed by an investigation into the structural properties of skew cyclic codes over $\mathcal{R}$. Later, we demonstrate that the Gray image of a skew cyclic code over $\mathcal{R}$ is a skew quasi-cyclic code. In Section 3.5, we provide the construction of quantum codes from dual-containing skew cyclic codes over $\mathcal{R}$. Finally, in Section 3.6, we study LCD codes over $\mathcal{R}$.

3.1 The Ring $\mathcal{R}$

Consider $\mathbb{F}_q[u_1, u_2, \ldots, u_r]/\langle u_i^3 - u_i, u_i u_j - u_j u_i\rangle$, which is a finite commutative ring. Let $T_1 = \mathbb{F}_q[u_1]\langle u_1^3 - u_1\rangle$ and $T_{j+1} = T_j[u_{j+1}]\langle u_{j+1}^3 - u_{j+1}\rangle$ then $\mathcal{R} = T_r$. Let

$$\mathcal{B}_j = \left\{\kappa_{j1} = 1 - u_j^2, \kappa_{j2} = \frac{u_j^2 - u_j}{2}, \kappa_{j3} = \frac{u_j^2 + u_j}{2}\right\}$$

Now let

$$\xi_{i_1 i_2 \ldots i_r} = \Pi_{j=1}^{r} \kappa_{j i_j}.$$

Then, we can verify that

$$\begin{aligned} \xi_{i_1 i_2 \ldots i_r}^2 &= \xi_{i_1 i_2 \ldots i_r} \\ \xi_{i_1 i_2 \ldots i_r} \xi_{l_1 l_2 \ldots l_r} &= 0 \\ \sum_{i_1, i_2, \ldots, i_r = 1}^{3} \xi_{i_1 i_2 \ldots i_r} &= 1, \end{aligned} \tag{3.1}$$

where $\sum_{i_1, i_2, \ldots, i_r = 1}^{3} = \sum_{i_1 = 1}^{3} \ldots \sum_{i_r = 1}^{3}$. Thus, by a decomposition theorem of ring theory 1.1.48,

$$\mathcal{R} = \bigoplus_{i_1, i_2, \ldots, i_r = 1}^{3} \xi_{i_1 i_2 \ldots i_r} \mathcal{R} \cong \bigoplus_{i_1, i_2, \ldots, i_r = 1}^{3} \xi_{i_1 i_2 \ldots i_r} \mathbb{F}_q.$$

Thus, any $\mathsf{v} \in \mathcal{R}$ can be expressed as

$$\mathsf{v} = \sum_{i_1, i_2, \ldots, i_r = 1}^{3} \xi_{i_1 i_2 \ldots i_r} v_{i_1 i_2 \ldots i_r}$$

in a unique way, where $v_{i_1 i_2 \ldots i_r} \in \mathbb{F}_q$ and $i_j \in \{1, 2, 3\}$ for $j = 1, 2, \ldots, r$.

3.2 Gray Map

We define a Gray map $\phi : \mathcal{R} \to \mathbb{F}_q^{3^r}$ as

$$\begin{aligned}\phi(\mathsf{v}) &= (v_{i_1 i_2 \ldots i_r})_{i_1,i_2,\ldots,i_r} M \\ &= (v_{11\ldots1}, \ldots, v_{11\ldots r}, v_{21\ldots1}, \ldots v_{33\ldots3}) M\end{aligned}$$

for all $\mathsf{v} = \sum_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1 i_2 \ldots i_r} v_{i_1 i_2 \ldots i_r} \in \mathcal{C}$, where $M \in GL_{3^r}(\mathbb{F}_q)$ is such that $MM^T = \lambda I_{3^r}$, for some $\lambda \in \mathbb{F}_q^*$. The Lee-weight of an element $\mathsf{v} \in \mathcal{R}$ is defined as

$$w_L(\mathsf{v}) = w_H(\phi(\mathsf{v})),$$

where w_H denotes the Hamming weight.

We can extend ϕ to $\mathcal{R}^n$ as $\Phi : \mathcal{R}^n \longrightarrow \mathbb{F}_q^{3^r n}$ as

$$\Phi(\mathbf{v}) = (\phi(\mathsf{v}^0), \phi(\mathsf{v}^1), \ldots, \phi(\mathsf{v}^{n-1})),$$

for all $\mathbf{v} = (\mathsf{v}^0, \mathsf{v}^1, \ldots, \mathsf{v}^{n-1}) \in \mathcal{R}^n$.

For any word $\mathbf{v} = (\mathsf{v}^0, \mathsf{v}^1, \ldots, \mathsf{v}^{n-1}) \in \mathcal{R}^n$, we define its Lee-weight as

$$w_L(\mathbf{v}) = \sum_{k=0}^{n-1} w_L(v^k).$$

And for any two words $\mathbf{v}, \mathbf{w} \in \mathcal{R}^n$, their Lee distance is define as

$$d_L(\mathbf{v}, \mathbf{w}) = w_L(\mathbf{v} - \mathbf{w}).$$

Theorem 3.2.1. The Gray map Φ is a bijective, linear map and it preserves the distance between $(\mathcal{R}^n, d_L)$ and $(\mathbb{F}_q^{3^r n}, d_H)$.

Proof. Since ϕ is bijective and linear, Φ is also bijective and linear. For the proof of later part, let $\mathbf{r}$ and $\mathbf{t} \in \mathcal{R}^n$ be such that

$$\mathbf{r} = (\mathsf{r}^0, \mathsf{r}^1, \ldots, \mathsf{r}^{n-1}),\ \mathbf{t} = (\mathsf{t}^0, \mathsf{t}^1, \ldots, \mathsf{t}^{n-1}),$$

where

$$\mathsf{r}^i = \sum_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1 i_2 \ldots i_r} r^i_{i_1 i_2 \ldots i_r},\ \mathsf{t}^i = \sum_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1 i_2 \ldots i_r} t^i_{i_1 i_2 \ldots i_r}$$

Now,

$$\begin{aligned}
d_L(\mathbf{r},\ \mathbf{t}) &= wt_L(\mathbf{r} - \mathbf{t}) \\
&= wt_L(\mathsf{r}^0 - \mathsf{t}^0, \mathsf{r}^1 - \mathsf{t}^1, \ldots, \mathsf{r}^{n-1} - \mathsf{t}^{n-1}) \\
&= \sum_{i=0}^{n-1} wt_L(\mathsf{r}^i - \mathsf{t}^i) \\
&= \sum_{i=0}^{n-1} wt_H(\phi(\mathsf{r}^i - \mathsf{t}^i)) \\
&= \sum_{i=0}^{n-1} wt_H(\phi(\mathsf{r}^i) - \phi(\mathsf{t}^i)) \\
&= wt_H(\phi(\mathsf{r}^0) - \phi(\mathsf{t}^0), \phi(\mathsf{r}^1) - \phi(\mathsf{t}^1), \ldots, \phi(\mathsf{r}^{n-1}) - \phi(\mathsf{t}^{n-1})) \\
&= wt_H((\phi(\mathsf{r}^0), \phi(\mathsf{r}^1), \ldots, \phi(\mathsf{r}^{n-1})) - (\phi(\mathsf{t}^0), \phi(\mathsf{t}^1), \ldots, \phi(\mathsf{t}^{n-1}))) \\
&= wt_H(\Phi(\mathbf{r}) - \Phi(\mathbf{t})) \\
&= d_H(\Phi(\mathbf{r}),\ \Phi(\mathbf{t}))
\end{aligned}$$

Hence, Φ is distance preserving between $(\mathcal{R}^n, d_L)$ and $(\mathbb{F}_q^{3^r n}, d_H)$. □

Theorem 3.2.2. For any two words $\mathbf{c}, \mathbf{d} \in \mathcal{R}^n$, $\mathbf{c} \perp \mathbf{d}$ if and only if $\Phi(\mathbf{c}) \perp \Phi(\mathbf{d})$. In other words, Φ preserves orthogonality.

Proof. Let $\mathbf{c}, \mathbf{d} \in \mathcal{R}^n$ such that $\mathbf{c} = (\mathsf{c}^0, \mathsf{c}^1, \ldots, \mathsf{c}^{n-1})$ and $\mathbf{d} = (\mathsf{d}^0, \mathsf{d}^1, \ldots, \mathsf{d}^{n-1})$, where $\mathsf{c}^i = \sum_{i_1,i_2,\ldots,i_r=1}^{3} c^i_{i_1 i_2 \ldots i_r} \xi_{i_1 i_2 \ldots i_r}$ and $\mathsf{d}^i = \sum_{i_1,i_2,\ldots,i_r=1}^{3} d^i_{i_1 i_2 \ldots i_r} \xi_{i_1 i_2 \ldots i_r}$, for $i =$

$0, 1, 2, \ldots, n-1$. Now, using the definition of Euclidean inner product and properties of primitive orthogonal idempotents, we get

$$\begin{aligned}
\mathbf{c}.\mathbf{d} &= \sum_{i=0}^{n-1} \mathsf{c}^i.\mathsf{d}^i \\
&= \sum_{i=0}^{n-1} \left(\sum_{i_1,i_2,\ldots,i_r=1}^{3} c^i_{i_1 i_2 \ldots i_r} \xi_{i_1 i_2 \ldots i_r} \right) \cdot \left(\sum_{l_1,l_2,\ldots,l_r=1}^{3} d^i_{l_1 l_2 \ldots l_r} \xi_{l_1,l_2,\ldots,l_r} \right) \\
&= \sum_{i=0}^{n-1} \left(\sum_{i_1,i_2,\ldots,i_r=1}^{3} c^i_{i_1 i_2 \ldots i_r} d^i_{i_1 i_2 \ldots i_r} \xi_{i_1 i_2 \ldots i_r} \right) \\
&= \sum_{i_1,i_2,\ldots,i_r=1}^{3} \left(\sum_{i=0}^{n-1} c^i_{i_1 i_2 \ldots i_r} d^i_{i_1 i_2 \ldots i_r} \right) \xi_{i_1 i_2 \ldots i_r}. \qquad (3.2)
\end{aligned}$$

and

$$\begin{aligned}
\Phi(\mathbf{c}).\Phi(\mathbf{d}) &= \Phi(\mathbf{c})\Phi(\mathbf{d})^T \\
&= \sum_{i=0}^{n-1} \phi(\mathsf{c}^i)\phi(\mathsf{d}^i)^T \\
&= \sum_{i=0}^{n-1} (c^i_{11\ldots1}, \ldots, c^i_{33\ldots3}) M M^T (d^i_{11\ldots1}, \ldots, d^i_{33\ldots3})^T \\
&= \lambda \sum_{i=0}^{n-1} \left(\sum_{i_1,i_2,\ldots,i_r=1}^{3} c^i_{i_1 i_2 \ldots i_r} d^i_{i_1 i_2 \ldots i_r} \right) \\
&= \lambda \sum_{i_1,i_2,\ldots,i_r=1}^{3} \sum_{i=0}^{n-1} c^i_{i_1 i_2 \ldots i_r} d^i_{i_1 i_2 \ldots i_r} \qquad (3.3)
\end{aligned}$$

Since, $\{\xi_{i_1 i_2 \ldots i_r} : i_j \in \{1, 2, 3\}\}$ is a linearly independent set and $\lambda \in \mathbb{F}_q^*$, from (3.2) and (3.3), we conclude that $\mathbf{c}.\mathbf{d} = 0$ if and only if $\Phi(\mathbf{c}).\Phi(\mathbf{d}) = 0$, i.e. $\mathbf{c} \perp \mathbf{d}$ if and only if $\Phi(\mathbf{c}) \perp \Phi(\mathbf{d})$. □

3.3 Linear Codes over $\mathcal{R}$

An $\mathcal{R}$-submodule of $\mathcal{R}^n$ is called a linear code over $\mathcal{R}$ of length n.

For a linear code $\mathcal{C} \subseteq \mathcal{R}^n$ and for $(i_1, i_2, \ldots, i_r) \in \{1,2,3\}^r$, we define

$$\mathcal{C}_{i_1 i_2 \ldots i_r} = \Bigg\{ \mathbf{w}_{i_1 i_2 \ldots i_r} \in \mathbb{F}_q^n \ : \exists\ \mathbf{w}_{k_1 k_2 \ldots k_r} \in \mathbb{F}_q^n, (k_1, k_2, \ldots, k_r) \in \{1,2,3\}^r \text{ and } (k_1, k_2, \ldots, k_r) \neq (i_1, i_2, \ldots, i_r) \text{ such that } \sum_{i_1, i_2, \ldots, i_r = 1}^{3} \xi_{i_1 i_2 \ldots i_r} \mathbf{w}_{i_1 i_2 \ldots i_r} \in \mathcal{C} \Bigg\}.$$

Then, $\mathcal{C}_{i_1 i_2 \ldots i_r} \subseteq \mathbb{F}_q^n$ is a linear code, $\forall\ i_j \in \{1,2,3\},\ j = 1, 2, \ldots, r$. Moreover, $\mathcal{C} = \bigoplus_{i_1, i_2, \ldots, i_r = 1}^{3} \xi_{i_1 i_2 \ldots i_r} \mathcal{C}_{i_1 i_2 \ldots i_r}$ and $|\mathcal{C}| = \prod_{i_1, i_2, \ldots, i_r = 1}^{3} |\mathcal{C}_{i_1 i_2 \ldots i_r}|$.

Definition 3.3.1. For a linear code $\mathcal{C}$ of length n over $\mathcal{R}$, its dual code $\mathcal{C}^\perp$ is defined as

$$\mathcal{C}^\perp = \{\mathbf{w} \in \mathcal{R}^n : \langle \mathbf{w}, \mathbf{v} \rangle = 0, \forall \mathbf{v} \in \mathcal{C}\},$$

where $\langle \mathbf{w}, \mathbf{v} \rangle$ denotes the usual Euclidean inner product on $\mathcal{R}^n$ defined as

$$\langle (\mathsf{w}^0, \mathsf{w}^1, \ldots, \mathsf{w}^{n-1}), (\mathsf{v}^0, \mathsf{v}^1, \ldots, \mathsf{v}^{n-1}) \rangle = \sum_{i=0}^{n-1} \mathsf{c}^i \mathsf{d}^i.$$

Definition 3.3.2. A linear code $\mathcal{C} \subseteq \mathcal{R}^n$ is called

(i) self-orthogonal if $\mathcal{C}^\perp \subseteq \mathcal{C}$,

(ii) dual-containing if $\mathcal{C} \subseteq \mathcal{C}^\perp$ and

(iii) self-dual if $\mathcal{C}^\perp = \mathcal{C}$.

Theorem 3.3.3. Let $\mathcal{C} = \bigoplus_{i_1, i_2, \ldots, i_r = 1}^{3} \xi_{i_1 i_2 \ldots i_r} \mathcal{C}_{i_1 i_2 \ldots i_r}$ be an (n, q^k, d_L) linear code over $\mathcal{R}$. Then,

(i) $\Phi(\mathcal{C})$ is a $[3^r n, k, d_H]$ linear code over $\mathbb{F}_q$, where $d_H = d_L$;

(ii) $\Phi(\mathcal{C})^{\perp} = \Phi(\mathcal{C}^{\perp})$;

(iii) $\mathcal{C}^{\perp} = \bigoplus_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1 i_2 \ldots i_r} \mathcal{C}^{\perp}_{i_1 i_2 \ldots i_r}$;

(iv) $\mathcal{C}$ is a self-orthogonal code if and only if $\Phi(\mathcal{C})$ is a self-orthogonal code over $\mathbb{F}_q$;

(v) $\mathcal{C}$ is a dual-containing code if and only if $\Phi(\mathcal{C})$ is a dual-containing code over $\mathbb{F}_q$;

(vi) $\mathcal{C}$ is a self-dual code if and only if $\Phi(\mathcal{C})$ is a self-dual code over $\mathbb{F}_q$.

Proof. (i) Clearly, length of $\Phi(\mathcal{C})$ is $3^r n$ as it is a subset of $\mathbb{F}_q^{3^r n}$. Furthermore, as Φ is bijective, we have $|\Phi(\mathcal{C})| = |\mathcal{C}| = q^k$. Therefore, $dim_{\mathbb{F}_q}\Phi(\mathcal{C}) = \log_q |\Phi(\mathcal{C})| = \log_q q^k = k$. By Theorem 3.2.1, $d_H = d_L$. Hence, $\Phi(\mathcal{C})$ is a $[3^r n, k, d_H]$ linear code over $\mathbb{F}_q$, where $d_H = d_L$.

(ii) Let $\mathbf{w} \in \Phi(\mathcal{C})^{\perp}$. Then, $\langle \mathbf{w}, \mathbf{v} \rangle = 0, \ \forall \ \mathbf{v} \in \Phi(\mathcal{C})$. Since Φ is bijective, we have $\langle \mathbf{w}, \Phi(\mathbf{u}) \rangle = 0, \ \forall \ \mathbf{u} \in \mathcal{C}$. Let $\mathbf{z} = \Phi^{-1}(\mathbf{w}) \in \mathcal{R}^n$. Thus, $\langle \Phi(\mathbf{z}), \Phi(\mathbf{u}) \rangle = 0, \ \forall \ \mathbf{u} \in \mathcal{C}$. Therefore, by Theorem 3.2.2, we have $\langle \mathbf{z}, \mathbf{u} \rangle = 0, \ \forall \ \mathbf{u} \in \mathcal{C}$. This shows that $\mathbf{z} \in \mathcal{C}^{\perp}$ and so $\mathbf{w} = \Phi(\mathbf{z}) \in \Phi(\mathcal{C}^{\perp})$. Therefore, $\Phi(\mathcal{C})^{\perp} \subseteq \Phi(\mathcal{C}^{\perp})$.

Conversely, let $\mathbf{w} \in \Phi(\mathcal{C}^{\perp})$. Then, $\exists!\ \mathbf{z} \in \mathcal{C}^{\perp}$ such that $\mathbf{w} = \Phi(\mathbf{z})$. Since Φ is bijective, we have $\langle \mathbf{z}, \Phi^{-1}(\mathbf{v}) \rangle = 0, \ \forall \ \mathbf{v} \in \Phi(\mathcal{C})$. Therefore, by Theorem 3.2.2, we have $\langle \Phi(\mathbf{z}), \mathbf{v} \rangle = \langle \mathbf{w}, \mathbf{v} \rangle = 0, \ \forall \ \mathbf{v} \in \Phi(\mathcal{C})$. This shows that $\mathbf{w} \in \Phi(\mathcal{C})^{\perp}$. Therefore, $\Phi(\mathcal{C}^{\perp}) \subseteq \Phi(\mathcal{C})^{\perp}$ as well. Hence, $\Phi(\mathcal{C}^{\perp}) = \Phi(\mathcal{C})^{\perp}$

(iii) Let $\mathcal{D} = \mathcal{C}^{\perp}$. Then,

$$\mathcal{D} = \left\{ \mathbf{w} \in \mathcal{R}^n \ : \langle \mathbf{w}, \mathbf{v} \rangle = 0, \forall \ \mathbf{v} \in \mathcal{C} \right\}.$$

$$= \Bigg\{ \mathbf{w} \in \mathcal{R}^n : \langle \mathbf{w}, \sum_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1 i_2 \ldots i_r} \mathbf{v}_{i_1 i_2 \ldots i_r} \rangle = 0,$$

$$\forall \ \mathbf{v}_{i_1 i_2 \ldots i_r} \in \mathcal{C}_{i_1 i_2 \ldots i_r}, i_j \in \{1,2,3\}, \ j = 1,2,\ldots,r \Bigg\}.$$

Now,

$$\mathcal{D}_{i_1i_2\ldots i_r} = \Big\{ \mathbf{w}_{i_1i_2\ldots i_r} \in \mathbb{F}_q^n \ : \exists\ \mathbf{w}_{k_1k_2\ldots k_r} \in \mathbb{F}_q^n, (k_1,k_2,\ldots,k_r) \in \{1,2,3\}^r \text{ and } (k_1,k_2,\ldots,k_r) \neq (i_1,i_2,\ldots,i_r) \text{ such that } \sum_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1i_2\ldots i_r}\mathbf{w}_{i_1i_2\ldots i_r} \in \mathcal{D} \Big\}.$$

$$= \Big\{ \mathbf{w}_{i_1i_2\ldots i_r} \in \mathbb{F}_q^n \ : \exists\ \mathbf{w}_{k_1k_2\ldots k_r} \in \mathbb{F}_q^n, (k_1,k_2,\ldots,k_r) \in \{1,2,3\}^r \text{ and } (k_1,k_2,\ldots,k_r) \neq (i_1,i_2,\ldots,i_r) \text{ such that } \left\langle \sum_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1i_2\ldots i_r}\mathbf{w}_{i_1i_2\ldots i_r}, \sum_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1i_2\ldots i_r}\mathbf{v}_{i_1i_2\ldots i_r} \right\rangle = 0 \Big\}.$$

$$= \Big\{ \mathbf{w}_{i_1i_2\ldots i_r} \in \mathbb{F}_q^n \ : \exists\ \mathbf{w}_{k_1k_2\ldots k_r} \in \mathbb{F}_q^n, (k_1,k_2,\ldots,k_r) \in \{1,2,3\}^r \text{ and } (k_1,k_2,\ldots,k_r) \neq (i_1,i_2,\ldots,i_r) \text{ such that } \sum_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1i_2\ldots i_r}\langle \mathbf{w}_{i_1i_2\ldots i_r}, \mathbf{v}_{i_1i_2\ldots i_r} \rangle = 0 \Big\}.$$

$$= \Big\{ \mathbf{w}_{i_1i_2\ldots i_r} \in \mathbb{F}_q^n \ : \exists\ \mathbf{w}_{k_1k_2\ldots k_r} \in \mathbb{F}_q^n, (k_1,k_2,\ldots,k_r) \in \{1,2,3\}^r \text{ and } (k_1,k_2,\ldots,k_r) \neq (i_1,i_2,\ldots,i_r) \text{ such that } \langle \mathbf{w}_{i_1i_2\ldots i_r}, \mathbf{v}_{i_1i_2\ldots i_r} \rangle = 0 \ \forall\ (k_1,k_2,\ldots,k_r) \in \{1,2,3\}^r, \text{ for any } \sum_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1i_2\ldots i_r}\mathbf{v}_{i_1i_2\ldots i_r} \in \mathcal{C} \Big\}.$$

$$= \mathcal{C}^{\perp}_{i_1i_2\ldots i_r}.$$

Hence, $\mathcal{C}^{\perp} = \bigoplus_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1i_2\ldots i_r}\mathcal{D}_{i_1i_2\ldots i_r} = \bigoplus_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1i_2\ldots i_r}\mathcal{C}^{\perp}_{i_1i_2\ldots i_r}$.

(iv) and (v) directly follow from the fact that for a bijective map Φ, $A \subseteq B \implies \Phi(A) \subseteq \Phi(B)$. Finally, (vi) follows by combining (iv).

□

Theorem 3.3.4. Let $\mathcal{C} = \bigoplus_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1i_2\ldots i_r}\mathcal{C}_{i_1i_2\ldots i_r}$ be a linear code of length n over $\mathcal{R}$. Furthermore, let $G_{i_1i_2\ldots i_r}$ be a generator matrix of $[n, k_{i_1i_2\ldots i_r}]$ q-ary linear code $\mathcal{C}_{i_1i_2\ldots i_r}$, $i_j \in \{1,2,3\}$, $j = 1,2,\ldots,r$ and M be the matrix used in Gray map

ϕ such that

$$G_{i_1i_2\ldots i_r} = \begin{bmatrix} a_{00}^{i_1i_2\ldots i_r} & a_{01}^{i_1i_2\ldots i_r} & \cdots & a_{0(n-1)}^{i_1i_2\ldots i_r} \\ a_{10}^{i_1i_2\ldots i_r} & a_{11}^{i_1i_2\ldots i_r} & \cdots & a_{1(n-1)}^{i_1i_2\ldots i_r} \\ \vdots & \vdots & \vdots & \vdots \\ a_{(k_{i_1i_2\ldots i_r}-1)0}^{i_1i_2\ldots i_r} & a_{(k_{i_1i_2\ldots i_r}-1)1}^{i_1i_2\ldots i_r} & \cdots & a_{(k_{i_1i_2\ldots i_r}-1)(n-1)}^{i_1i_2\ldots i_r} \end{bmatrix}_{k_{i_1i_2\ldots i_r}\times n}$$

$$\text{and } M = \begin{bmatrix} m_{11\ldots11,11\ldots11} & \cdots & m_{11\ldots11,33\ldots33} \\ \vdots & \vdots & \vdots \\ m_{33\ldots33,11\ldots11} & \cdots & m_{33\ldots33,33\ldots33} \end{bmatrix}_{3^r\times 3^r} \in GL_{3^r}(\mathbb{F}_q).$$

Then,

$$G = \begin{bmatrix} G_{11\ldots11}\otimes M_{R_{11\ldots11}} \\ G_{11\ldots12}\otimes M_{R_{11\ldots12}} \\ \vdots \\ G_{33\ldots33}\otimes M_{R_{33\ldots33}} \end{bmatrix}$$

is a generator matrix of $\Phi(\mathcal{C})$, where $M_{R_{i_1i_2\ldots i_r}}$ denotes the $i_1i_2\ldots i_r{}^{th}$ row of M, $i_j \in \{1,2,3\},\ j = 1,2,\ldots,r$.

Proof. Let $\mathbf{w} \in \Phi(\mathcal{C})$ be an arbitrary element. Since, Φ is bijective, there exists a unique codeword $\mathbf{v} = \sum_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1i_2\ldots i_r}\mathbf{v}_{i_1i_2\ldots i_r} \in \mathcal{C}$ such that $\Phi(\mathbf{v}) = \mathbf{w}$ and $\mathbf{v}_{i_1i_2\ldots i_r} = (\mathsf{v}_{i_1i_2\ldots i_r}^0, \mathsf{v}_{i_1i_2\ldots i_r}^1, \ldots, \mathsf{v}_{i_1i_2\ldots i_r}^{n-1}) \in \mathcal{C}_{i_1i_2\ldots i_r}$. Since, $G_{i_1i_2\ldots i_r}$ is a generator matrix of $\mathcal{C}_{i_1i_2\ldots i_r}$, there exist $\alpha_{i_1i_2\ldots i_r,0}, \alpha_{i_1i_2\ldots i_r,1}, \ldots, \alpha_{i_1i_2\ldots i_r,k_{i_1i_2\ldots i_r}-1}$ such that

$$\begin{aligned} \mathbf{v}_{i_1i_2\ldots i_r} &= \sum_{l=0}^{k_{i_1i_2\ldots i_r}-1} \alpha_{i_1i_2\ldots i_r,l}\left(a_{l0}^{i_1i_2\ldots i_r}, a_{l1}^{i_1i_2\ldots i_r}, \ldots, a_{l(n-1)}^{i_1i_2\ldots i_r}\right) \\ &= \left(\sum_{l=0}^{k_{i_1i_2\ldots i_r}-1} \alpha_{i_1i_2\ldots i_r,,l}a_{l0}^{i_1i_2\ldots i_r}, \sum_{l=0}^{k_{i_1i_2\ldots i_r}-1} \alpha_{i_1i_2\ldots i_r,,l}a_{l1}^{i_1i_2\ldots i_r}, \ldots,\right. \end{aligned}$$

$$\sum_{l=0}^{k_{i_1 i_2 \ldots i_r}-1} \alpha_{i_1 i_2 \ldots i_r,,l} a_{l(n-1)}^{i_1 i_2 \ldots i_r} \Bigg).$$

Then,

$$\begin{aligned}
\mathbf{v} &= \sum_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1 i_2 \ldots i_r} \mathbf{v}_{i_1 i_2 \ldots i_r} \\
&= \sum_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1 i_2 \ldots i_r} \Bigg(\sum_{l=0}^{k_{i_1 i_2 \ldots i_r}-1} \alpha_{i_1 i_2 \ldots i_r,l} a_{l0}^{i_1 i_2 \ldots i_r}, \sum_{l=0}^{k_{i_1 i_2 \ldots i_r}-1} \alpha_{i_1 i_2 \ldots i_r,l} a_{l1}^{i_1 i_2 \ldots i_r}, \ldots, \\
&\qquad \sum_{l=0}^{k_{i_1 i_2 \ldots i_r}-1} \alpha_{i_1 i_2 \ldots i_r,l} a_{l(n-1)}^{i_1 i_2 \ldots i_r} \Bigg) \\
&= \Bigg(\sum_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1 i_2 \ldots i_r} \Bigg(\sum_{l=0}^{k_{i_1 i_2 \ldots i_r}-1} \alpha_{i_1 i_2 \ldots i_r,l} a_{l0}^{i_1 i_2 \ldots i_r} \Bigg), \\
&\qquad \sum_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1 i_2 \ldots i_r} \Bigg(\sum_{l=0}^{k_{i_1 i_2 \ldots i_r}-1} \alpha_{i_1 i_2 \ldots i_r,l} a_{l1}^{i_1 i_2 \ldots i_r} \Bigg), \ldots, \\
&\qquad \sum_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1 i_2 \ldots i_r} \Bigg(\sum_{l=0}^{k_{i_1 i_2 \ldots i_r}-1} \alpha_{i_1 i_2 \ldots i_r,l} a_{l(n-1)}^{i_1 i_2 \ldots i_r} \Bigg) \Bigg) \\
&= (\mathtt{v}^0, \mathtt{v}^1, \ldots, \mathtt{v}^{n-1}) \text{ (say)}.
\end{aligned}$$

Therefore, $\mathbf{w} = \Phi(\mathbf{v}) = (\phi(\mathtt{v}^0), \phi(\mathtt{v}^1), \ldots, \phi(\mathtt{v}^{n-1})) = (\mathtt{w}^0, \mathtt{w}^1, \ldots, \mathtt{w}^{n-1})$ (say). Then,

$$\begin{aligned}
\mathtt{w}^i &= \phi \Bigg(\sum_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1 i_2 \ldots i_r} \Bigg(\sum_{l=0}^{k_{i_1 i_2 \ldots i_r}-1} \alpha_{i_1 i_2 \ldots i_r,l} a_{li}^{i_1 i_2 \ldots i_r} \Bigg) \Bigg) \\
&= \Bigg(\sum_{l=0}^{k_{11\ldots11}-1} \alpha_{11\ldots11,l} a_{li}^{11\ldots11}, \sum_{l=0}^{k_{11\ldots12}-1} \alpha_{11\ldots12,l} a_{li}^{11\ldots12}, \ldots, \\
&\qquad \sum_{l=0}^{k_{33\ldots33}-1} \alpha_{33\ldots33,l} a_{li}^{33\ldots33} \Bigg) M \\
&= \Bigg(\sum_{i_1,i_2,\ldots,i_r=1}^{3} m_{i_1 i_2 \ldots i_r,11\ldots11} \Bigg(\sum_{l=0}^{k_{i_1 i_2 \ldots i_r}-1} \alpha_{i_1 i_2 \ldots i_r,l} a_{li}^{i_1 i_2 \ldots i_r} \Bigg),
\end{aligned}$$

$$\sum_{i_1,i_2,\ldots,i_r=1}^{3} m_{i_1i_2\ldots i_r,11\ldots12}\left(\sum_{l=0}^{k_{i_1i_2\ldots i_r}-1}\alpha_{i_1i_2\ldots i_r,l}a_{li}^{i_1i_2\ldots i_r}\right),\ldots,$$
$$\sum_{i_1,i_2,\ldots,i_r=1}^{3} m_{i_1i_2\ldots i_r,l_1l_2\ldots l_r}\left(\sum_{l=0}^{k_{i_1i_2\ldots i_r}-1}\alpha_{i_1i_2\ldots i_r,l}a_{li}^{i_1i_2\ldots i_r}\right)\Bigg)$$

$= \mathbf{a}\mathcal{G}^i$ (say).

$$\mathbf{a} = \begin{bmatrix}\alpha_{11\ldots11,0} & \ldots & \alpha_{11\ldots11,k_{11\ldots11}-1} & \ldots & \alpha_{33\ldots33,0} & \ldots & \alpha_{33\ldots33,k_{33\ldots33}-1}\end{bmatrix}$$

$$\mathcal{G}^i = \begin{bmatrix} m_{11\ldots11,11\ldots11}a_{0i}^{11\ldots11} & \ldots & m_{11\ldots11,33\ldots33}a_{0i}^{11\ldots11} \\ m_{11\ldots11,11\ldots11}a_{1i}^{11\ldots11} & \ldots & m_{11\ldots11,33\ldots33}a_{1i}^{11\ldots11} \\ \vdots & \vdots & \vdots \\ m_{11\ldots11,11\ldots11}a_{(k_{11\ldots11}-1)i}^{11\ldots11} & \ldots & m_{11\ldots11,33\ldots33}a_{(k_{11\ldots11}-1)i}^{11\ldots11} \\ \vdots & \vdots & \vdots \\ m_{33\ldots33,11\ldots11}a_{0i}^{33\ldots33} & \ldots & m_{33\ldots33,33\ldots33}a_{0i}^{33\ldots33} \\ m_{33\ldots33,11\ldots11}a_{1i}^{33\ldots33} & \ldots & m_{33\ldots33,33\ldots33}a_{1i}^{33\ldots33} \\ \vdots & \vdots & \vdots \\ m_{33\ldots33,11\ldots11}a_{(k_{33\ldots33}-1)i}^{33\ldots33} & \ldots & m_{33\ldots33,33\ldots33}a_{(k_{33\ldots33}-1)i}^{33\ldots33} \end{bmatrix}$$

$$= \begin{bmatrix} G_{11\ldots11,C_i}\otimes M_{R_{11\ldots11}} \\ G_{11\ldots12,C_i}\otimes M_{R_{11\ldots12}} \\ \vdots \\ G_{33\ldots33,C_i}\otimes M_{R_{33\ldots33}} \end{bmatrix},$$

where $G_{i_1i_2\ldots i_r,C_i}$ denotes the i^{th} column of $G_{i_1i_2\ldots i_r}$, and $M_{R_{i_1i_2\ldots i_r}}$ denotes the $i_1i_2\ldots i_r{}^{th}$ row of M. Thus,

$$\mathbf{w} = (\mathsf{w}^0, \mathsf{w}^1, \ldots, \mathsf{w}^{n-1})$$
$$= \mathbf{a}\begin{bmatrix}\mathcal{G}^0 & \mathcal{G}^1 & \ldots & \mathcal{G}^{n-1}\end{bmatrix} = G \text{ (say)}.$$

Hence,

$$G = \begin{bmatrix}\mathcal{G}^0 & \mathcal{G}^1 & \ldots & \mathcal{G}^{n-1}\end{bmatrix}$$

$$= \begin{bmatrix} G_{11\ldots11,C_0} \otimes M_{R_{11\ldots11}} & \ldots & G_{11\ldots11,C_{n-1}} \otimes M_{R_{11\ldots11}} \\ G_{11\ldots12,C_0} \otimes M_{R_{11\ldots12}} & \ldots & G_{11\ldots12,C_{n-1}} \otimes M_{R_{11\ldots12}} \\ \vdots & \vdots & \vdots \\ G_{33\ldots33,C_0} \otimes M_{R_{33\ldots33}} & \ldots & G_{33\ldots33,C_{n-1}} \otimes M_{R_{33\ldots33}} \end{bmatrix}$$

$$= \begin{bmatrix} G_{11\ldots11} \otimes M_{R_{11\ldots11}} \\ G_{11\ldots12} \otimes M_{R_{11\ldots12}} \\ G_{33\ldots33} \otimes M_{R_{33\ldots33}} \end{bmatrix} \text{ is a generator matrix of } \Phi(\mathcal{C}).$$

□

3.4 Skew Cyclic Codes over $\mathcal{R}$

Let $\Theta : \mathcal{R} \to \mathcal{R}$ be an automorphism. Then $\Theta|_{\mathbb{F}_q}$, the restriction map over $\mathbb{F}_q$ is an $\mathbb{F}_q$-automorphism. Therefore, $\Theta|_{\mathbb{F}_q} = \theta_t : a \longmapsto a^{p^t}$ for some t such that $0 \leq t \leq m-1$, where $q = p^m$ and $a \in \mathbb{F}_q$. Thus, for $\sum_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1 i_2 \ldots i_r} v_{i_1 i_2 \ldots i_r} \in \mathcal{R}$, we have

$$\Theta\left(\sum_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1 i_2 \ldots i_r} v_{i_1 i_2 \ldots i_r}\right) = \sum_{i_1,i_2,\ldots,i_r=1}^{3} \Theta\left(\xi_{i_1 i_2 \ldots i_r}\right) v_{i_1 i_2 \ldots i_r}^{p^t}.$$

From eq. 3.1, we conclude that the set $\{\xi_{i_1 i_2 \ldots i_r} : i_j \in \{1,2,3\},\ j = 1,2,\ldots,r\}$ is a complete set in $\mathcal{R}$. Therefore, the set $\{\Theta(\xi_{i_1 i_2 \ldots i_r}) : i_j \in \{1,2,3\}\ for\ j = 1,2,\ldots,r\}$ is permutation of the set $\{\xi_{i_1 i_2 \ldots i_r} : i_j \in \{1,2,3\},\ j = 1,2,\ldots,r\}$. Hence, $\exists\ \gamma_j \in S_3$, the permutation group of $\{1,2,3\}$, for $j = 1,2,\ldots,r$ such that $\Theta(\xi_{i_1 i_2 \ldots i_r}) = \xi_{\gamma_1(i_1)\gamma_2(i_2)\ldots\gamma_r(i_r)}$. Therefore,

$$\Theta\left(\sum_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1 i_2 \ldots i_r} v_{i_1 i_2 \ldots i_r}\right) = \sum_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{\gamma_1(i_1)\gamma_2(i_2)\ldots\gamma_r(i_r)} v_{i_1 i_2 \ldots i_r}^{p^t}.$$

If $\gamma_j = id$ (the identity permutation), for all $j = 1, 2, \ldots, r$ and $\Theta|_{\mathbb{F}_q} = \theta_t$, then Θ will be denoted as Θ_t.

Definition 3.4.1. Let $\Theta \in Aut(\mathcal{R})$ and $\sigma_\Theta : \mathcal{R}^n \longrightarrow \mathcal{R}^n$ be defined as

$$\mathbf{v} = (\mathsf{v}^0, \mathsf{v}^1, \ldots, \mathsf{v}^{n-1}) \longmapsto (\Theta(\mathsf{v}^{n-1}), \Theta(\mathsf{v}^0), \ldots, \Theta(\mathsf{v}^{n-2})).$$

A linear code $\mathcal{C} \subseteq \mathcal{R}^n$ such that $\sigma_\Theta(\mathbf{v}) \in \mathcal{C}$, whenever $\mathbf{v} \in \mathcal{C}$ is called a skew Θ-cyclic code of length n over $\mathcal{R}$.

For an automorphism Θ of $\mathcal{R}$, $\mathcal{R}[y;\Theta]$ is a non-commutative ring (in general) under the usual addition of polynomials and multiplication defined as $y * ay = \Theta(a)y^2$ and it is called skew-Θ polynomial ring. Moreover, for a vector $\mathbf{v} = (\mathsf{v}^0, \mathsf{v}^1, \ldots, \mathsf{v}^{n-1}) \in \mathcal{R}^n, \mathbf{v} \mapsto \sum_{i=0}^{n-1} \mathsf{v}^i y^i$ is an isomorphism between $\mathcal{R}^n$ and $\mathcal{R}[y;\Theta]/\langle y^n - 1\rangle$. Under this isomorphism, a linear code C is a skew Θ-cyclic code of length n if and only if it (its image) is a left submodule of $A_n = \mathcal{R}[y;\Theta]/\langle y^n - 1\rangle$. If the order of Θ divides n then A_n is a ring and a linear code C is a skew Θ-cyclic code of length n if and only if it (its image) is a left ideal of A_n.

Theorem 3.4.2. Let $\Theta_t \in Aut(\mathbb{F}_q)$ and $\mathcal{C} = \bigoplus_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1 i_2 \ldots i_r} \mathcal{C}_{i_1 i_2 \ldots i_r}$ be a linear code of length n over $\mathcal{R}$. Then, $\mathcal{C}$ is a skew Θ_t-cyclic code over $\mathcal{R}$ if and only if $\mathcal{C}_{i_1 i_2 \ldots i_r}$ is a skew θ_t-cyclic code over $\mathbb{F}_q$, for all $i_j \in \{1, 2, 3\},\ j = 1, 2, \ldots, r$.

Proof. Let $\mathbf{c} = (\mathsf{c}^0, \mathsf{c}^1, \mathsf{c}^2, \ldots, \mathsf{c}^{n-1}) \in \mathcal{C}$ be an arbitrary codeword. For $l \in \{0, 1, \ldots, n-1\}$, let $\mathsf{c}^l = \sum_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1 i_2 \ldots i_r} c^l_{i_1 i_2 \ldots i_r}$. Then, $\mathbf{c}_{i_1 i_2 \ldots i_r} = \left(c^0_{i_1 i_2 \ldots i_r}, c^1_{i_1 i_2 \ldots i_r}, \ldots, c^{n-1}_{i_1 i_2 \ldots i_r}\right) \in \mathcal{C}_{i_1 i_2 \ldots i_r}$. Now,

$$\begin{aligned}
&\sigma_{\Theta_t}(\mathbf{c}) \\
&= \left(\Theta_t(\mathsf{c}^{n-1}), \Theta_t(\mathsf{c}^0), \Theta_t(\mathsf{c}^1), \ldots, \Theta_t(\mathsf{c}^{n-2})\right) \\
&= \left(\sum_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1 i_2 \ldots i_r} \theta_t(c^{n-1}_{i_1 i_2 \ldots i_r}), \sum_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1 i_2 \ldots i_r} \theta_t(c^0_{i_1 i_2 \ldots i_r}), \ldots, \right.
\end{aligned}$$

$$\left. \sum_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1 i_2 \ldots i_r} \theta_t(c^{n-2}_{i_1 i_2 \ldots i_r}) \right)$$

$$= \left(\sum_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1 i_2 \ldots i_r}(\theta_t(c^{n-1}_{i_1 i_2 \ldots i_r})), \sum_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1 i_2 \ldots i_r} \theta_t(c^{0}_{i_1 i_2 \ldots i_r}), \ldots, \right.$$

$$\left. \sum_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1 i_2 \ldots i_r} \theta_t(c^{n-2}_{i_1 i_2 \ldots i_r}) \right)$$

$$= \sum_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1 i_2 \ldots i_r} \left(\theta_t(c^{n-1}_{i_1 i_2 \ldots i_r}), \theta_t(c^{0}_{i_1 i_2 \ldots i_r}), \theta_t(c^{1}_{i_1 i_2 \ldots i_r}), \ldots, \theta_t(c^{n-2}_{i_1 i_2 \ldots i_r}) \right)$$

$$= \sum_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1 i_2 \ldots i_r} \left(\sigma_{\theta_t}(c^{0}_{i_1 i_2 \ldots i_r}, c^{1}_{i_1 i_2 \ldots i_r}, \ldots, c^{n-1}_{i_1 i_2 \ldots i_r}) \right)$$

$$= \sum_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1 i_2 \ldots i_r} \left(\sigma_{\theta_t}(\mathbf{c}_{i_1 i_2 \ldots i_r}) \right).$$

By the unique representation of elements of $\mathcal{C}$ as a linear combination of elements of $\mathcal{C}_{i_1 i_2 \ldots i_r}$, we conclude that $\sigma_{\Theta_t}(\mathbf{c}) \in \mathcal{C}$ if and only if $\sigma_{\theta_t}(\mathbf{c}_{i_1 i_2 \ldots i_r}) \in \mathcal{C}_{i_1 i_2 \ldots i_r}$, for all $i_j \in \{1, 2, 3\},\ j = 1, 2, \ldots r$. Hence, $\mathcal{C}$ is a skew Θ_t-cyclic code over $\mathcal{R}$ if and only if $\mathcal{C}_{i_1 i_2 \ldots i_r}$ is a skew θ_t-cyclic code over $\mathbb{F}_q$, for all $i_j \in \{1, 2, 3\},\ j = 1, 2, \ldots r$. □

Theorem 3.4.3. Let $\mathcal{C} = \bigoplus_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1 i_2 \ldots i_r} \mathcal{C}_{i_1 i_2 \ldots i_r}$ be a skew Θ_t-cyclic code of length n over $\mathcal{R}$. Let $\mathcal{C}_{i_1 i_2 \ldots i_r} = \langle f_{i_1 i_2 \ldots i_r}(y) \rangle$, where $f_{i_1 i_2 \ldots i_r}(y)$ are monic right divisors of $y^n - 1$ and $i_j \in \{1, 2, 3\}$, for $j = 1, 2, \ldots, r$. Then, $\exists$ a polynomial $f(y)$ in $\mathcal{R}[y; \Theta_t]$ such that

(i) $\mathcal{C} = \langle f(y) \rangle$,

(ii) $f(y)$ is right divisor of $y^n - 1$ and

(iii) $|\mathcal{C}| = q^{3^r n - \sum_{i_1,i_2,\ldots,i_r=1}^{3} deg(f_{i_1 i_2 \ldots i_r}(y))}$.

Proof. Since $\mathcal{C} = \bigoplus_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1 i_2 \ldots i_r} \mathcal{C}_{i_1 i_2 \ldots i_r}$ and $\mathcal{C}_{i_1 i_2 \ldots i_r} = \langle f_{i_1 i_2 \ldots i_r}(y) \rangle$, $i_j \in \{1, 2, 3\}$, $j = 1, 2, \ldots, r$, we have

$$\mathcal{C} = \left\{ c(y) = \sum_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1 i_2 \ldots i_r} r_{i_1 i_2 \ldots i_r}(y) f_{i_1 i_2 \ldots i_r}(y) | r_{i_1 i_2 \ldots i_r}(y) \in \mathbb{F}_q[y; \theta_t] \right\}.$$

Hence, $\mathcal{C} \subseteq \langle \xi_{11\ldots1} f_{11\ldots1}(y), \ldots, \xi_{33\ldots3} f_{33\ldots3}(y) \rangle$. Conversely, for any

$$\sum_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1 i_2 \ldots i_r} k_{i_1 i_2 \ldots i_r}(y) f_{i_1 i_2 \ldots i_r}(y) \in \langle \xi_{11\ldots1} f_{11\ldots1}(y), \ldots, \xi_{33\ldots3} f_{33\ldots3}(y) \rangle,$$

where $k_{i_1 i_2 \ldots i_r}(y) \in \mathbb{F}_q[y; \theta_t] / \langle y^n - 1 \rangle$, there exist $r_{i_1 i_2 \ldots i_r}(y) \in \mathbb{F}_q[y; \theta_t]$ such that

$$\xi_{i_1 i_2 \ldots i_r} k_{i_1 i_2 \ldots i_r}(y) = \xi_{i_1 i_2 \ldots i_r} r_{i_1 i_2 \ldots i_r}(y).$$

Thus, $\langle \xi_{11\ldots1} f_{11\ldots1}(y), \ldots, \xi_{33\ldots3} f_{33\ldots3}(y) \rangle \subseteq \mathcal{C}$. Hence

$$\langle \xi_{11\ldots1} f_{11\ldots1}(y), \ldots, \xi_{33\ldots3} g_{33\ldots3}(y) \rangle = \mathcal{C}.$$

Now, let $f(y) = \sum_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1 i_2 \ldots i_r} f_{i_1 i_2 \ldots i_r}(y)$ then $\langle f(y) \rangle \subseteq \mathcal{C}$. Also since $\xi_{i_1 i_2 \ldots i_r} f_{i_1 i_2 \ldots i_r} = \xi_{i_1 i_2 \ldots i_r} f_{i_1 i_2 \ldots i_r}$, for all $i_j \in \{1, 2, 3\}$ so $\mathcal{C} \subseteq \langle f(y) \rangle$. Hence $\mathcal{C} \subseteq \langle f(y) \rangle$. Further as $f_{i_1 i_2 \ldots i_r}(y)$ divides $y^n - 1 \in \mathbb{F}_q[y : \theta_t]$ and are monic as well for all $i_j \in \{1, 2, 3\}$. Thus, $y^n - 1 = g_{i_1 i_2 \ldots i_r}(y) f_{i_1 i_2 \ldots i_r}(y)$ for some $g_{i_1 i_2 \ldots i_r}(y) \in \mathbb{F}_q[y; \theta_t]$. Therefore,

$$\begin{aligned}
&\left(\sum_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1 i_2 \ldots i_r} g_{i_1 i_2 \ldots i_r}(y) \right) f(y) \\
&= \left(\sum_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1 i_2 \ldots i_r} g_{i_1 i_2 \ldots i_r}(y) \right) \left(\sum_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1 i_2 \ldots i_r} f_{i_1 i_2 \ldots i_r}(y) \right) \\
&= \sum_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1 i_2 \ldots i_r} g_{i_1 i_2 \ldots i_r}(y) f_{i_1 i_2 \ldots i_r}(y)
\end{aligned}$$

$$= \sum_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1 i_2 \ldots i_r}(y^n - 1)$$

$$= y^n - 1 \in \mathcal{R}[y; \Theta_t].$$

Hence, $f(y)$ divides $y^n - 1$ from right. Since $|\mathcal{C}| = \Pi_{i_1 i_2 \ldots i_r} |\mathcal{C}_{i_1 i_2 \ldots i_r}|$, we get

$$|\mathcal{C}| = q^{3^r n - \sum_{i_1,i_2,\ldots,i_r=1}^{3} deg(f_{i_1 i_2 \ldots i_r}(y))}.$$

□

Example 3.4.4. Let $q = 5^2$ then $\mathbb{F}_q = GF[5]/\langle X^2 + 4X + 2\rangle$ and let s be a root of $X^2 + 4X + 2$. Consider the ring $\mathbb{F}_q/\langle u_1^3 - u_1, u_2^3 - u_2, u_1 u_2 - u_2 u_1\rangle$. Let $\theta = \theta_1$ be the Frobenius map i.e.

$$a \longmapsto a^5.$$

Then the order of θ is 2. Now consider the factorization of $x^4 - 1$ in $\mathbb{F}_q[x; \theta]$.

$$\begin{aligned} y^4 - 1 &= (y + 2s + 1)(y + 2s + 2)(y + 4s + 4)(y + 4s + 2) \\ &= (y + 4)(y + 1)(y + 2)(y + 3) \\ &= (y + 2s + 1)(y + 2s + 2)(y + 3)(y + 2) \\ &= (y + 2s + 1)(y + 2s + 2)(y + s + 1)(y + s + 3) \end{aligned}$$

Let $f(y) = (y + 4s + 4)(y + 4s + 2) = y^2 + (s + 1)y + 1$ which is a right divisor of $y^4 - 1$. Then for all $i_j \in \{1, 2, 3\}$, let $\mathcal{C}_{i_1 i_2 \ldots i_r} = \langle f(x)\rangle$ is a skew cyclic code. A generator matrix of $\mathcal{C}_{i_1 i_2 \ldots i_r}$ is given as:

$$\begin{bmatrix} 1 & s+1 & 1 & 0 \\ 0 & 1 & 4s^2 + 2 & 1 \end{bmatrix}$$

$\mathcal{C}_{i_1 i_2 \ldots i_r}$ are $[4, 2, 3]$ skew cyclic codes over $\mathbb{F}_q$ which is MDS. Hence, we have $\mathcal{C} = \bigoplus_{i_1, i_2, \ldots, i_r = 1}^{3} \xi_{i_1 i_2 \ldots i_r} \mathcal{C}_{i_1 i_2 \ldots i_r}$ is a skew cyclic code of length 4 over $\mathcal{R}$ with minimum Lee distance $d_L = 3$.

Theorem 3.4.5. A skew Θ-cyclic code $\mathcal{C} \subseteq \mathcal{R}^n$ is a quasi-cyclic code of index ν, where $\nu = \frac{n}{(n, o(\theta))}$.

Proof. Let $n_\Theta = (n, O(\Theta))$ and $n = n_\Theta l$. By extended Euclidean algorithm, we find two integers c' and d' satisfying $n_\theta = c' O(\Theta) + d' n$. If $d' > 0$, find $e \in \mathbb{N}$ satisfying $O(\Theta)e - d' > 0$. Then $(c' + ne)O(\Theta) = n_\Theta + (O(\Theta)e - d')n$. In this case, take $c = c' + ne$ and $d = O(\Theta)e - d'$. Otherwise if $d' < 0$, then simply take $c = c'$ and $d = -d'$. Thus we have $cO(\Theta) = n_\Theta + dn$. Let

$$\mathbf{w} = (w_{0,0}, w_{0,1}, \ldots, w_{0,n_\Theta - 1}, w_{1,0}, w_{1,1}, \ldots, w_{1,n_\Theta - 1}, \ldots, w_{l-1,0}, w_{l-1,1}, \ldots, w_{l-1,n_\Theta - 1}) \in \mathcal{C}.$$

Say, $\mathbf{w} = (\mathsf{w}^0, \mathsf{w}^1, \ldots, \mathsf{w}^{l-1})$, where $\mathsf{w}^i = (w_{i,0}, w_{i,1}, \ldots, w_{i,n_\theta - 1})$. Now since $\mathcal{C}$ is a skew cyclic code, $\sigma_\Theta(\mathbf{w}), \sigma_\Theta^2(\mathbf{w}), \ldots, \sigma_\Theta^{n_\Theta}(\mathbf{w}), \ldots, \sigma_\Theta^{n_\theta + dn}(\mathbf{w}), \ldots \in \mathcal{C}$. Since $n_\Theta + dn$ is divisible by $O(\Theta)$, we have

$$\begin{aligned}
\sigma_\Theta^{n_\Theta + dn} &= (\Theta^{n_\Theta + dn}(\mathsf{w}^{l-1}), \Theta^{n_\Theta + dn}(\mathsf{w}^0), \Theta^{n_\Theta + dn}(\mathsf{w}^1), \ldots, \Theta^{n_\Theta + dn}(\mathsf{w}^{l-2})) \\
&= (\mathsf{w}^{l-1}, \mathsf{w}^0, \ldots, \mathsf{w}^{l-2}) \\
&= \tau_{id,l}(\mathbf{w}) \in \mathcal{C}
\end{aligned}$$

This shows that $\forall\ \mathbf{w} \in \mathcal{C}$, $\tau_{id,l}(\mathbf{w}) \in \mathcal{C}$. Hence, $\mathcal{C}$ is a quasi-cyclic code of index l. In particular, if $n_\Theta = 1$, then $n = l$ and so $\mathcal{C}$ is cyclic. □

Corollary 3.4.6. Let $(n, O(\Theta_t)) = 1$ and $y^n - 1 = \prod_{k=1}^{s} f_k(y)^{n_k}$, where $f_k(y)$ are irreducible factors. Then the number of skew θ_t-cyclic codes of length n over $\mathcal{R}$ is $\prod_{k=1}^{s} (n_k + 1)^{3^r}$.

Example 3.4.7. Let $q = 3^4$ then $\mathbb{F}_q = GF[3]/\langle X^4+2X^3+2\rangle = \mathbb{F}_3(\beta)$ where β is a root of X^4+2X^3+2. Further, let $r = 3$. Then $\mathcal{R} = T_3 = \mathbb{F}_{81}/\langle u_1^3-u_1, u_2^3-u_2, u^3-u_3, u_1u_2-u_2u_1, u_1u_3-u_3u_1, u_2u_3-u_3u_2\rangle$. Let Θ_1 be an automorphism of $\mathcal{R}$ such that $\Theta_1(\xi_{i_1i_2i_3}) = \xi_{\gamma_1(i_1)\gamma_2(i_2)\gamma_3(i_3)}$ where $\gamma_1 = (23), \gamma_2 = (123)$ and $\gamma_3 = (132) \in S_3$ the permutation group of $\{1,2,3\}$ and $\Theta_1|_{\mathbb{F}_{81}} = \theta_1$ the Frobenius map i.e. $\theta_1 : a \longmapsto a^3$. Then the order of θ_1 is 4 and that of Θ_1, $O(\Theta_1) = lcm(2,3,3,4) = 12$. Now let $n = 24$ and then from the factorization of $y^{24}-1$ in $\mathbb{F}_{81}[x;\theta_1]$ we observe that $u(y) = y^{17}+(\beta^2+\beta+1)y^{16}+2y^{13}+(2\beta^2+2\beta+2)y^{12}+y^5+(\beta^2+\beta+1)y^4+2y+2\beta^2+2\beta+2$ is a right divisor of $y^{24}-1$. Let $\mathcal{C}_{i_1i_2i_3} = \langle u(y)\rangle$ for all $i_j \in \{1,2,3\}$. Thus $\mathcal{C}_{i_1i_2i_3}$ is a skew θ_1-cyclic code of length 24 and minimum distance 6. Since $gcd(24,12) = 12 > 1$. Hence by Theorem 3.4 skew Θ_1-cyclic code $\mathcal{C} = \bigoplus_{i_1i_2i_3} \xi_{i_1i_2i_3}\mathcal{C}_{i_1i_2i_3}$ is a quasi-cyclic code of index $2(= 24/12)$ and $d_L = 6$.

Again Let Θ_2 be another automorphism of $\mathcal{R}$ such that $\Theta_2(\xi_{i_1i_2i_3}) = \xi_{\gamma_1(i_1)\gamma_2(i_2)\gamma_3(i_3)}$ where $\gamma_1 = \gamma_2 = \gamma_3 = id$, the identity permutation and $\Theta_2|_{\mathbb{F}_{81}} = \theta_1$ the Frobenius map i.e. $\theta_1 : a \longmapsto a^3$. Then $O(\Theta_2) = lcm(1,1,1,4) = 4$. Suppose that $n = 15$ then $gcd(15,4) = 1$ and hence by Theorem 3.4 any skew Θ_2-cyclic code is cyclic. Thus y^n-1 has a unique factorization as:

$$y^{15}-1 = (y^4+y^3+y^2+y+1)^3(y+2)^3.$$

Hence by Corollary 3.4.6, there are $(3+1)^{27} \times (3+1)^{27} = 4^{54}$ skew Θ_2-cyclic codes over $\mathcal{R}$ in total.

Finally Let Θ_3 be an automorphism of $\mathcal{R}$ where $\gamma_1 = (12), \gamma_2 = (13)$ and $\gamma_3 = (23) \in S_3$ and $\Theta_3|_{\mathbb{F}_{81}} = \theta_2$ i.e. $\theta_2 : a \longmapsto a^{3^2} = a^9$. Now $o(\gamma_1) = o(\gamma_2) = o(\gamma_3) = o(\theta_2) = 2$ and so $O(\Theta_3) = lcm(2,2,2,2) = 2$. If we take $n = 8$ then by Theorem 3.4, any skew Θ_3-cyclic code is a quasi-cyclic code of index 4 and any skew Θ_3-cyclic code over $\mathcal{R}$ of odd length is cyclic.

Example 3.4.8. Let $q = 5^3$ then $\mathbb{F}_q = GF[5]/\langle X^3+3X+3\rangle = \mathbb{F}_3(\delta)$ where δ is a root of X^3+3X+3. Further, let $r = 2$. Then $\mathcal{R} = T_2 = \mathbb{F}_{125}/\langle u_1^3-u_1, u_2^3-u_2, u_1u_2-u_2u_1\rangle$. Let Θ_1 be an automorphism of $\mathcal{R}$ such that $\Theta_1(\xi_{i_1i_2i_3}) = \xi_{\gamma_1(i_1)\gamma_2(i_2)\gamma_3(i_3)}$ where $\gamma_1 = (123), \gamma_2 = (132)$ and $\gamma_3 = (123) \in S_3$ the permutation group of $\{1, 2, 3\}$ and $\Theta_1|_{\mathbb{F}_{125}} = \theta_1$ the Frobenius map i.e. $\theta_1 : a \longmapsto a^5$. Then the order of θ_1 is 3 and that of Θ_1, $O(\Theta_1) = lcm(3, 3, 3, 3) = 3$. Now let $n = 18$ and then from the factorization of $y^{18} - 1$ in $\mathbb{F}_{125}[x; \theta_1]$ we observe that $u(y) = y^{12} + y^9 + 4y^3 + 4$ is a right divisor of $y^{18} - 1$. Let $\mathcal{C}_{i_1i_2i_3} = \langle u(y)\rangle$ for all $i_j \in \{1, 2, 3\}$. Thus $\mathcal{C}_{i_1i_2i_3}$ is a skew θ_1-cyclic code of length 18 and minimum distance 4. Since $gcd(18, 3) = 3 > 1$. Hence by Theorem 3.4, the skew Θ_1-cyclic code $\mathcal{C} = \bigoplus_{i_1i_2i_3} \xi_{i_1i_2i_3}\mathcal{C}_{i_1i_2i_3}$ is a quasi-cyclic code of index $6(= 18/3)$ and $d_L = 4$.

Let Θ_2 be another automorphism of $\mathcal{R}$ such that $\Theta_2(\xi_{i_1i_2i_3}) = \xi_{\gamma_1(i_1)\gamma_2(i_2)\gamma_3(i_3)}$ where $\gamma_1 = \gamma_2 = \gamma_3 = id$, the identity permutation and $\Theta_2|_{\mathbb{F}_{125}} = \theta_2$ i.e. $\theta_2 : a \longmapsto a^{10}$. Then $O(\Theta_2) = lcm(1, 1, 1, 3) = 3$. Suppose that $n = 20$ then $gcd(20, 3) = 1$ and hence by Theorem 3.4, any skew Θ_2-cyclic code is cyclic. Thus $y^n - 1$ has a unique factorization as:

$$y^{20} - 1 = (y + 4)^5(y + 2)^5(y + 3)^5(y + 1)^5.$$

Hence by Corollary 3.4.6, there are $(5 + 1)^9 \times (5 + 1)^9 \times (5 + 1)^9 \times (5 + 1)^9 = 6^{36}$ skew Θ_2-cyclic codes over $\mathcal{R}$ in total.

3.5 Construction of Quantum Codes from Skew Cyclic Codes over $\mathcal{R}$

The focus of this section is on building quantum codes from skew cyclic codes over $\mathcal{R}$. We begin by revisiting the definition of quantum codes and the CSS construction. We also revisit a criterion for identifying dual-containing skew cyclic codes over $\mathbb{F}_q$, which we leverage to characterize dual-containing skew cyclic codes over $\mathcal{R}$. We then present an approach to generate quantum codes from dual-containing skew cyclic codes over $\mathcal{R}$, and we use this method to construct a novel quantum code.

Theorem 3.5.1. Let $\Theta \in Aut(\mathcal{R})$ and n be a multiple of $o(\Theta)$. Then, the dual code of a skew Θ-cyclic code $\mathcal{C}$, denoted as $\mathcal{C}^{\perp}$ is also a skew Θ-cyclic code.

Proof. Let $\mathbf{c} = (\mathsf{c}^0, \mathsf{c}^1, \ldots, \mathsf{c}^{n-1}) \in \mathcal{C}$ and $\mathbf{d} = (\mathsf{d}^0, \mathsf{d}^1, \ldots, \mathsf{d}^{n-1}) \in \mathcal{C}^{\perp}$ be arbitrary elements. Since, $\mathcal{C}$ is given to be a skew Θ-cyclic code, we have $\sigma_{\Theta}^{n-1}(\mathbf{c}) \in \mathcal{C}$. Therefore,

$$\begin{aligned} 0 &= \langle \sigma_{\Theta}^{n-1}(\mathbf{c}), \mathbf{d} \rangle \\ &= \sum_{i=1}^{n-1} \Theta^{n-1}(\mathsf{c}^i)\mathsf{d}^{i-1} + \Theta^{n-1}(\mathsf{c}^0)\mathsf{d}^{n-1}. \end{aligned}$$

Applying Θ on both sides and using the assumption that n is a multiple of $o(\Theta)$, we get

$$\begin{aligned} 0 &= \sum_{i=1}^{n-1} \mathsf{c}^i \Theta(\mathsf{d}^{i-1}) + \mathsf{c}^0 \Theta(\mathsf{d}^{n-1}) \\ &= \langle (\mathsf{c}^0, \mathsf{c}^1, \ldots, \mathsf{c}^{n-1}), (\Theta(\mathsf{d}^{n-1}), \Theta(\mathsf{d}^0), \ldots, \Theta(\mathsf{d}^{n-2})) \rangle \\ &= \langle \mathbf{c}, \sigma_{\Theta}(\mathbf{d}) \rangle. \end{aligned}$$

Since, $\mathbf{c} \in \mathcal{C}$ is arbitrary, we have $\sigma_\Theta(\mathbf{d}) \in \mathcal{C}^\perp$. Thus, $\sigma_\Theta(\mathbf{d}) \in \mathcal{C}^\perp$ whenever $\mathbf{d} \in \mathcal{C}^\perp$. Hence, $\mathcal{C}^\perp$ is a skew Θ-cyclic code. □

Definition 3.5.2. The left monic skew reciprocal polynomial of $g(y) = \sum_{j=0}^{\ell} g_j y^j \in \mathbb{F}_q[y;\theta]$, $g_o \neq 0$ is defined as $g^\dagger(y) = \frac{1}{\theta^\ell(g_0)}(\sum_{j=0}^{\ell} \theta^j(g_{\ell-j})y^j)$.

Lemma 3.5.3. ([31, Corollary 5.7]) Let C be skew θ-cyclic code of length n over $\mathbb{F}_q$ such that $ord(\theta) \mid n$. If $f(y)$ is the generator polynomial of C such that $g(y)f(y) = y^n - 1$. Then, C contains its dual if and only if $g^\dagger(y)g(y)$ is divisible by $y^n - 1$ from the right.

Theorem 3.5.4. Let $\mathcal{C} = \bigoplus_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1 i_2 \ldots i_r} \mathcal{C}_{i_1 i_2 \ldots i_r}$ be a skew Θ_t-cyclic code of length n over $\mathcal{R}$ such that $ord(\Theta_t) \mid n$ and $f_{i_1 i_2 \ldots i_r}(y)$ is the generator polynomial of $\mathcal{C}_{i_1 i_2 \ldots i_r}$ and $g_{i_1 i_2 \ldots i_r}(y) f_{i_1 i_2 \ldots i_r}(y) = y^n - 1, \forall\ i_j \in \{1,2,3\},\ j = 1,2,\ldots,r$.

(i) $\mathcal{C}$ contains its dual if and only if $g^\dagger_{i_1 i_2 \ldots i_r}(y) g_{i_1 i_2 \ldots i_r}(y)$ is divisible by $y^n - 1$ from right, $\forall\ i_j \in \{1,2,3\},\ j = 1,2,\ldots,r$.

(ii) If $g^\dagger_{i_1 i_2 \ldots i_r}(y) g_{i_1 i_2 \ldots i_r}(y)$ is divisible by $y^n - 1$ from right, $\forall\ i_j \in \{1,2,3\}$, then there exists an $[[N,K,D]]_q$ quantum code, where $N = 3^r n$, $K = 3^r n - 2\sum_{i_1,i_2,\ldots,i_r=1}^{3} deg(f_{i_1 i_2 \ldots i_r}(y))$, and $D \geq d_L$, the Lee distance of $\mathcal{C}$.

Proof. (i) Let us suppose that $\mathcal{C}^\perp \subseteq \mathcal{C}$. Then, by Theorem 3.3.3 (iii), we get

$$\bigoplus_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1 i_2 \ldots i_r} \mathcal{C}^\perp_{i_1 i_2 \ldots i_r} \subseteq \bigoplus_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1 i_2 \ldots i_r} \mathcal{C}_{i_1 i_2 \ldots i_r}.$$

Now, taking modulo $\xi_{i_1 i_2 \ldots i_r}$ both sides, we get $\mathcal{C}^\perp_{i_1 i_2 \ldots i_r} \subseteq \mathcal{C}_{i_1 i_2 \ldots i_r}$, for all $i_j \in \{1,2,3\},\ j = 1,2,\ldots,r$. Then, by Lemma 3.5.3, $g^\dagger_{i_1 i_2 \ldots i_r}(y) g_{i_1 i_2 \ldots i_r}(y)$ is divisible by $y^n - 1$ from right, $\forall\ i_j \in \{1,2,3\},\ j = 1,2,\ldots,r$. Conversely, if $g^\dagger_{i_1 i_2 \ldots i_r}(y) g_{i_1 i_2 \ldots i_r}(y)$ is divisible by $y^n - 1$ from right, $\forall\ i_j \in \{1,2,3\},\ j =$

$1, 2, \ldots, r$ then, again by Lemma 3.5.3, $\mathcal{C}^{\perp}_{i_1 i_2 \ldots i_r} \subseteq \mathcal{C}_{i_1 i_2 \ldots i_r}$, for all $i_j \in \{1, 2, 3\}$, $j = 1, 2, \ldots, r$. Thus, $\bigoplus_{i_1, i_2, \ldots, i_r = 1}^{3} \xi_{i_1 i_2 \ldots i_r} \mathcal{C}^{\perp}_{i_1 i_2 \ldots i_r} \subseteq \bigoplus_{i_1, i_2, \ldots, i_r = 1}^{3} \xi_{i_1 i_2 \ldots i_r} \mathcal{C}_{i_1 i_2 \ldots i_r}$ and hence by Theorem 3.3.3 (iii), $\mathcal{C}^{\perp} \subseteq \mathcal{C}$.

(ii) Let $g^{\dagger}_{i_1 i_2 \ldots i_r}(y) g_{i_1 i_2 \ldots i_r}(y)$ be divisible by $y^n - 1$ from right, $\forall\ i_j \in \{1, 2, 3\}$, $j = 1, 2, \ldots, r$. Then, by part (i), we have $\mathcal{C}^{\perp} \subseteq \mathcal{C}$. Therefore, by Theorem 3.3.3 (ii), we have $\Phi(\mathcal{C})^{\perp} = \Phi(\mathcal{C}^{\perp}) \subseteq \Phi(\mathcal{C})$. Then, by Theorems 3.2.1 and (i) and 4.2.8, $\Phi(\mathcal{C})$ is a $[3^r n, 3^r n - \sum_{i_1, i_2, \ldots, i_r = 1}^{3} deg(f_{i_1 i_2 \ldots i_r}(y)),\ d_L]$ dual-containing skew quasi-cyclic code over $\mathbb{F}_q$. Hence, by Lemma 1.3.6, there exists an $[[N, K, D]]_q$ quantum code, where $N = 3^r n$, $K = 3^r n - 2 \sum_{i_1, i_2, \ldots, i_r = 1}^{3} deg(f_{i_1 i_2 \ldots i_r}(y))$, and $D \geq d_L$, the Lee distance of $\mathcal{C}$.

□

Example 3.5.5. Let $q = 25$ and $r = 1$ then $\mathcal{R} = \mathbb{F}_{25}/\langle u_1^3 - u_1 \rangle$. Let θ_1 be the Frobenius automorphism and $\gamma_1 = id$ the identity permutation. So $\Theta : \mathcal{R} \to \mathcal{R}$ defined as

$$w_1\xi_1 + w_2\xi_2 + w_3\xi_3 \longmapsto w_1^5\xi_1 + w_2^5\xi_2 + w_3^5\xi_3$$

is an automorphism. Let $n = 8$. Consider two factorisations of $y^n - 1 \in \mathbb{F}_{25}[y; \theta_1]$ as:

$y^8-1 = (y+3w+3)(y+3w+4)(y+w+2)^2(y+4w+2)(y+4w+4)(y+4w+1)(y+4w) =$
$(y+2w+1)(y+2w+2)(y+2w)(y+2w+3)(y+4w+1)(y+w+1)(y+2w+4)(y+3)$,
where w is a primitive of $\mathbb{F}_{25}$.

Let us take $f_1(y) = y + 4w$, $f_2(y) = 1$ and $f_3(y) = (y + 2w + 4)(y + 3) = y^2 + (2w + 2)y + w + 2$ and $y^n - 1 = g_i(y) f_i(y)$. Then $g_i^*(y) g_i(y)$ is divisible by $y^n - 1$ for all $i = 1, 2, 3$. Take

$$M = \begin{bmatrix} 3 & 3 & 1 \\ 1 & 3 & 3 \\ 2 & 4 & 2 \end{bmatrix}$$

then $MM^T = 4I_3$. Let $\mathcal{C}_i = \langle f_i(y) \rangle$ and $\mathcal{C} = \bigoplus_{i=1}^{3} \xi_i \mathcal{C}_i$ then $\Phi(\mathcal{C})$ is a dual-containing $[24, 21, 3]_{25}$ code. Hence by Theorem 3.5.4, there exists a $[[24, 18, 3]]_{25}$ quantum code which is a new code as per database [9].

Finally, we'll conclude this section by enlisting some quantum codes in Tables 3.1, 3.2 and 3.3 constructed using Theorem 3.5.4.

TABLE 3.1: Quantum Codes from Skew Cyclic Codes over $\mathbb{F}_q[u_1]/\langle u_1^3 - u_1\rangle$

q	n	$f_1(y)$	$f_2(y)$	$f_3(y)$	$\Phi(\mathcal{C})$	$[[n,k,d]]_q$	Remark
27	6	$w1$	21	$w^{21}w^{12}1$	$[18,14,4]$	$[[18,10,4]]_{27}$	new
27	9	$w^{25}1$	$w^7w^{10}w^{19}1$	$1w^{25}1$	$[27,21,5]$	$[[27,15,5]]_{27}$	new
27	9	$w^2w^{22}1$	$w^5w^{20}w^5 1$	$1w^{25}1$	$[27,20,6]$	$[[27,13,6]]_{27}$	new

TABLE 3.2: Quantum Codes from Skew Cyclic Codes over $\mathbb{F}_q[u_1,u_2]/\langle u_1^3 - u_1, u_2^3 - u_2, u_1u_2 - u_2u_1\rangle$

q	n	$f_{11}(y)$	$f_{12}(y)$	$f_{13}(y)$	$f_{21}(y)$	$f_{22}(y)$	$f_{23}(y)$	$f_{31}(y)$	$f_{32}(y)$	$f_{33}(y)$	$\Phi(\mathcal{C})$	$[[n,k,d]]_q$	Remark
27	6	11	1	1	$w1$	1	11	1	1	$w^{21}w^{12}1$	$[54,49,3]$	$[[54,44,3]]_{27}$	new
27	6	11	1	1	$w1$	1	11	1	$w^{21}w^{12}1$	$w1$	$[54,48,4]$	$[[54,42,4]]_{27}$	new

TABLE 3.3: Quantum Codes from Skew Cyclic Codes over $\mathbb{F}_q[u_1, u_2, u_3]/\langle u_1^3 - u_1, u_2^3 - u_2, u_3^3 - u_3, u_iu_j - u_ju_i\rangle$

q	n	$f_{111}(y)$	$f_{112}(y)$	$f_{113}(y)$	$f_{121}(y)$	$f_{122}(y)$	$f_{123}(y)$	$f_{131}(y)$	$f_{132}(y)$	$f_{133}(y)$	$f_{211}(y)$	$f_{212}(y)$	$f_{213}(y)$	$f_{221}(y)$	$f_{222}(y)$	$f_{223}(y)$
27	6	11	1	1	1	1	1	1	1	1	1	$w1$	1	1	1	1
27	6	11	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Table 3.3 continued

$f_{231}(y)$	$f_{232}(y)$	$f_{233}(y)$	$f_{311}(y)$	$f_{312}(y)$	$f_{313}(y)$	$f_{321}(y)$	$f_{322}(y)$	$f_{323}(y)$	$f_{331}(y)$	$f_{332}(y)$	$f_{333}(y)$	$\Phi(\mathcal{C})$	$[[n, k, d]]_q$	Remark
1	1	1	1	1	1	1	$w1$	1	1	$w^{21}w^{12}1$	21	$[162, 156, 4]_{27}$	$[[162, 150, 4]]$	new
1	1	1	1	1	1	1	$w1$	1	1	$w^{21}w^{12}1$	21	$[162, 157, 4]$	$[[162, 152, 3]]_{27}$	new

3.6 LCD Codes over $\mathcal{R}$

In this section, our focus is on LCD codes over $\mathcal{R}$. We begin by reviewing essential criteria established by Boulanour et al. [20] that identify when a skew cyclic code over a finite field is LCD. We then present a technique for deriving LCD codes from skew cyclic codes over $\mathcal{R}$, based on these criteria and a decomposition method for skew cyclic codes. The section concludes with illustrative examples.

Definition 3.6.1. ([69]) A linear code $\mathcal{C}$ whose Hull is trivial (zero submodule), is called a Linear Complementary Dual (LCD) code, where $\text{Hull}(\mathcal{C}) := \mathcal{C} \cap \mathcal{C}^{\perp}$.

In [20], Boulanour et al. provided a criterion for skew constacyclic codes to be LCD. We state a particular case ($\lambda = 1$) of Theorem 2 from [20].

Lemma 3.6.2. ([20, Theorem 2]) Let θ_t be an automorphism of $\mathbb{F}_q$ and C be a skew θ_t cyclic code of length n over $\mathbb{F}_q$ such that $f \in \mathbb{F}_q[y;\theta_t]$ is generator polynomial of C. Further assume that $g \in \mathbb{F}_q[y;\theta_t]$ is such that $\theta_t^n(g).f = y^n - 1$. Then C is Euclidean LCD if and only if $GCRD(f, g^{\dagger}) = 1$, where, $g^{\dagger}$ denotes the left monic skew reciprocal polynomial of g defined as $g^{\dagger}(y) = \frac{1}{\theta^{\ell}(g_0)}(\sum_{j=0}^{\ell} \theta^j(g_{\ell-j})y^j)$ if $g(y) = \sum_{j=0}^{\ell} g_j y^j \in \mathbb{F}_q[y;\theta]$, $g_o \neq 0$.

Theorem 3.6.3. Let $\mathcal{C} = \bigoplus_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1 i_2 \ldots i_r} \mathcal{C}_{i_1 i_2 \ldots i_r}$ be a linear code of length n over $\mathcal{R}$. Then, $\mathcal{C}$ is an LCD if and only if $\mathcal{C}_{i_1 i_2 \ldots i_r}$ is an LCD code of length n over $\mathbb{F}_q$, $\forall\ i_j \in \{1,2,3\},\ j = 1,2,\ldots,r$.

Proof. Since, $\mathcal{C}^{\perp} = \bigoplus_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1 i_2 \ldots i_r} \mathcal{C}_{i_1 i_2 \ldots i_r}^{\perp}$, we have

$$\begin{aligned}
\mathcal{C} \cap \mathcal{C}^{\perp} &= \Big(\bigoplus_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1 i_2 \ldots i_r} \mathcal{C}_{i_1 i_2 \ldots i_r} \Big) \cap \Big(\bigoplus_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1 i_2 \ldots i_r} \mathcal{C}_{i_1 i_2 \ldots i_r} \Big)^{\perp} \\
&= \left(\bigoplus_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1 i_2 \ldots i_r} \mathcal{C}_{i_1 i_2 \ldots i_r} \right) \cap \left(\bigoplus_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1 i_2 \ldots i_r} \mathcal{C}_{i_1 i_2 \ldots i_r}^{\perp} \right)
\end{aligned}$$

$$= \bigoplus_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1 i_2 \ldots i_r} \left(\mathcal{C}_{i_1 i_2 \ldots i_r} \cap \mathcal{C}_{i_1 i_2 \ldots i_r}^{\perp} \right)$$

Thus, $Hull(\mathcal{C}) = \{0\}$ if and only if $Hull(\mathcal{C}_{i_1 i_2 \ldots i_r}) = \{0\}$ $\forall$ $i_j \in \{1, 2, 3\}$. Hence, $\mathcal{C}$ is an LCD if and only if $\mathcal{C}_{i_1 i_2 \ldots i_r}$ is an LCD code of length n over $\mathbb{F}_q$, $\forall$ $i_j \in \{1, 2, 3\}$, $j = 1, 2, \ldots, r$. □

Theorem 3.6.4. Let order of Θ_t divides n and $\mathcal{C} = \bigoplus_{i_1,i_2,\ldots,i_r=1}^{3} \xi_{i_1 i_2 \ldots i_r} \mathcal{C}_{i_1 i_2 \ldots i_r}$ be a skew Θ_t-cyclic code of length n over $\mathcal{R}$ and $f_{i_1 i_2 \ldots i_r}(y)$ be the generator polynomial of $\mathcal{C}_{i_1 i_2 \ldots i_r}$, for $i_j \in \{1, 2, 3\}$. Further assume that $g_{i_1 i_2 \ldots i_r} \in \mathbb{F}_q[y; \theta_t]$ is such that $g_{i_1 i_2 \ldots i_r}(y).f_{i_1 i_2 \ldots i_r}(y) = y^n - 1$. Then, C is LCD if and only if $GCRD(f_{i_1 i_2 \ldots i_r}, g_{i_1 i_2 \ldots i_r}^{\dagger}) = 1$.

Proof. Combining Lemma 3.6.2 and Theorem 3.6.3, the proof follows. □

Lemma 3.6.5. For a linear code $\mathcal{C}$ of length n over $\mathcal{R}$, $\Phi(Hull(\mathcal{C})) = Hull(\Phi(\mathcal{C}))$.

Proof. Let $\mathbf{w} \in \Phi(Hull(\mathcal{C}))$. Since Φ is onto, $\exists$ $\mathbf{v} \in Hull(\mathcal{C})$ such that $\Phi(\mathbf{v}) = \mathbf{w})$. As $\mathbf{v} \in Hull(\mathcal{C})$, $\mathbf{v} \in \mathcal{C}$ and $\mathbf{v} \in \mathcal{C}^{\perp}$. Therefore, $\mathbf{w} \in \Phi(\mathcal{C})$, and $\mathbf{w} \in \Phi(\mathcal{C}^{\perp})$ and so $\mathbf{w} \in \Phi(\mathcal{C}) \cap \Phi(\mathcal{C}^{\perp})$. Since, $\mathbf{w} \in \Phi(\mathcal{C} \cap \mathcal{C}^{\perp})$ is arbitrary, we have, $\Phi(Hull(\mathcal{C})) \subseteq Hull(\Phi(\mathcal{C}))$.

Again let $\mathbf{w} \in Hull(\Phi(\mathcal{C}))$, i.e. $\mathbf{w} \in \Phi(\mathcal{C})$, and $\mathbf{w} \in \Phi(\mathcal{C}^{\perp})$. Then $\exists$ $\mathbf{u} \in \mathcal{C}$ and $\exists$ $\mathbf{v} \in \mathcal{C}^{\perp}$ such that $\Phi(\mathbf{u}) = \mathbf{w})$ and $\Phi(\mathbf{v}) = \mathbf{w})$. Since, Φ is one-one as well, we have, $\mathbf{u} = \mathbf{v}$ and so $\mathbf{u}(= \mathbf{v}) \in \mathcal{C} \cap \mathcal{C}^{\perp}$. Therefore, $\mathbf{w} \in \Phi(\mathcal{C} \cap \mathcal{C}^{\perp})$. Since, $\mathbf{w} \in \Phi(\mathcal{C}) \cap \Phi(\mathcal{C}^{\perp})$ is arbitrary, we have, $Hull(\Phi(\mathcal{C})) \subseteq \Phi(Hull(\mathcal{C}))$. Hence, $\Phi(Hull(\mathcal{C})) = Hull(\Phi(\mathcal{C}))$.. □

Theorem 3.6.6. A linear code of length n over $\mathcal{R}$ is LCD code if and only if its Gray image is a q-ary LCD code of length $3^r n$.

Proof. Suppose that $\mathcal{C}$ is an LCD code of length n over the ring $\mathcal{R}$. Then by definition, $Hull(\mathcal{C}) = \{0\}$. By Lemma 3.6.5, we get $Hull(\Phi(\mathcal{C})) = \Phi(Hull(\mathcal{C})) = \Phi(\{0\}) = \{0\}$ which concludes that $\Phi(\mathcal{C})$ is an LCD of length $3^r n$ over $\mathcal{R}$. Conversely, suppose that $\Phi(\mathcal{C})$ is an LCD of length $3^r n$ over $\mathbb{F}_q$ then $Hull(\Phi(\mathcal{C})) = \{0\}$. Therefore, by Lemma 3.6.5, we have $\Phi(Hull(\mathcal{C})) = Hull(\Phi(\mathcal{C})) = \{0\}$ which implies that $\mathcal{C} \cap \mathcal{C}^{\perp} = \{0\}$, as Φ is one-one. Hence, $\mathcal{C}$ is an LCD code of length n over $\mathcal{R}$. □

Now, we utilize the results obtained in this section to provide some examples of LCD codes over $\mathcal{R}$. For computation purposes, SageMath [90] and MAGMA [23, 17] software are used.

Example 3.6.7. Let $q = 25$ and $r = 2$ then $\mathcal{R} = \mathbb{F}_{25}/\langle u_1^3 - u_1, u_2^3 - u_2, u_1u_2 - u_1u_2 \rangle$. Let θ_1 be the Frobenius automorphism and $\gamma_1 = id$ the identity permutation. So $\Theta_1 : \mathcal{R} \to \mathcal{R}$ defined as

$$\sum_{i_1 i_2} w_{i_1 i_2} \xi_{i_1 i_2} \longmapsto \sum_{i_1 i_2} w_{i_1 i_2}^5 \xi_{i_1 i_2}$$

is an automorphism. Take

$$M = \begin{bmatrix} 2 & 1 & 1 & 2 & 1 & 1 & 4 & 2 & 2 \\ 4 & 3 & 4 & 4 & 3 & 4 & 3 & 1 & 3 \\ 1 & 1 & 2 & 1 & 1 & 2 & 2 & 2 & 4 \\ 4 & 2 & 2 & 2 & 1 & 1 & 2 & 1 & 1 \\ 3 & 1 & 3 & 4 & 3 & 4 & 4 & 3 & 4 \\ 2 & 2 & 4 & 1 & 1 & 2 & 1 & 1 & 2 \\ 3 & 4 & 4 & 1 & 3 & 3 & 3 & 4 & 4 \\ 1 & 2 & 1 & 2 & 4 & 2 & 1 & 2 & 1 \\ 4 & 4 & 3 & 3 & 3 & 1 & 4 & 4 & 3 \end{bmatrix}$$

then $MM^T = I_9$. Let $n = 4$. Factorisation of $y^n - 1 \in \mathbb{F}_{25}[y; \theta_1]$ is given as:

$$y^n - 1 = (y + 1)(y + 4)(y + 3)(y + 2)$$

Let us take $f_{11}(y) = y + 1$ and $f_{i_1 i_2}(y) = 1$ if $(i_1, i_2) \neq (1, 1)$ and $y^n - 1 = g_{i_1 i_2}(y) f_{i_1 i_2}(y)$. Then $GCRD(g^{\dagger}_{i_1 i_2}(y), f_{i_1 i_2}(y)) = 1$. Let $\mathcal{C}_i = \langle f_i(y) \rangle$ and $\mathcal{C} = \bigoplus_{i=1}^{3} \xi_i \mathcal{C}_i$ then $\mathcal{C}$ is an LCD code of length $n = 4$ and $d_L = 2$ over $\mathcal{R}$. Hence $\Phi(\mathcal{C})$ is a $[36, 35, 2]$ LCD code over $\mathbb{F}_{25}$ which is MDS.

Finally, we'll conclude this section by enlisting some LCD codes over $\mathcal{R}$ in Tables 3.4, 3.5, 3.6.

TABLE 3.4: LCD Codes from Skew Cyclic Codes over $\mathbb{F}_q[u_1]/\langle u_1^3 - u_1\rangle$

q	n	$f_1(y)$	$f_2(y)$	$f_3(y)$	$\Phi(\mathcal{C})$	Remark
9	4	$w^3 1$	$w^3 w^6 1$	11	$[12, 8, 4]$	AMDS, BKLC
9	4	$w^4 01$	$w^3 1$	$w^5 w^7 1$	$[12, 7, 5]$	AMDS, BKLC
9	8	$w^3 1$	$w^5 1$	$w^4 w^6 1$	$[24, 20, 4]$	AMDS, BKLC
9	8	$w w^5 11$	$w w^7 211$	$w^7 w^7 w^6 1$	$[24, 14, 8]$	BKLC
9	8	$w w^2 w^7 1$	$w^3 1$	$w^7 w^7 w^2 01$	$[24, 16, 6]$	BKLC
25	4	$w^{16} 1$	1	$w^{22} 1$	$[12, 10, 3]$	MDS
25	6	11	$w^4 1$	141	$[18, 4, 4]$	AMDS
27	6	$w^{25} 1$	$w^2 1$	$w^{24} 1$	$[18, 15, 3]$	AMDS
27	6	$w^7 1$	$w01$	$w^{17} 1$	$[18, 14, 4]$	AMDS

TABLE 3.5: LCD Codes from Skew Cyclic Codes over $\mathbb{F}_q[u_1, u_2]/\langle u_1^3 - u_1, u_2^3 - u_2, u_1u_2 - u_2u_1\rangle$

q	n	$f_{11}(y)$	$f_{12}(y)$	$f_{13}(y)$	$f_{21}(y)$	$f_{22}(y)$	$f_{23}(y)$	$f_{31}(y)$	$f_{32}(y)$	$f_{33}(y)$	$\Phi(\mathcal{C})$	Remark
9	4	11	1	1	1	1	11	1	1	$w1$	$[36, 33, 3]$	AMDS, BKLC
9	4	$w^7 1$	1	1	1	1	$w^7 1$	1	1	11	$[36, 33, 3]$	AMDS, BKLC
9	4	11	1	1	1	1	11	1	1	$w^3 1$	$[36, 33, 3]$	AMDS, BKLC
9	4	11	1	1	1	1	11	1	1	$w^7 1$	$[36, 33, 3]$	AMDS, BKLC
9	4	$w1$	1	11	1	$w1$	1	$w^7 1$	1	$w^5 1$	$[36, 31, 4]$	BKLC
9	4	$w1$	1	11	1	$w1$	1	$w^5 1$	1	$w^5 1$	$[36, 31, 4]$	BKLC
9	4	$w^3 1$	1	11	1	$w1$	1	$w^3 1$	1	$w^3 1$	$[36, 31, 4]$	BKLC
25	4	11	1	1	1	1	11	1	1	$w^2 1$	$[36, 33, 3]$	AMDS, BKLC

TABLE 3.6: LCD Codes from Skew Cyclic Codes over $\mathbb{F}_q[u_1, u_2, u_3]/\langle u_1^3 - u_1, u_2^3 - u_2, u_3^3 - u_3, u_iu_j - u_ju_i\rangle$

q	n	$f_{111}(y)$	$f_{112}(y)$	$f_{113}(y)$	$f_{121}(y)$	$f_{122}(y)$	$f_{123}(y)$	$f_{131}(y)$	$f_{132}(y)$	$f_{133}(y)$	$f_{211}(y)$	$f_{212}(y)$	$f_{213}(y)$	$f_{221}(y)$	$f_{222}(y)$	$f_{223}(y)$
9	4	11	1	1	1	1	1	1	1	1	$w1$	1	1	1	1	1
25	4	$w^{16} 1$	1	1	1	1	1	1	1	1	$w^2 1$	1	1	1	1	1

Table 3.6 continued

$f_{231}(y)$	$f_{232}(y)$	$f_{233}(y)$	$f_{311}(y)$	$f_{312}(y)$	$f_{313}(y)$	$f_{321}(y)$	$f_{322}(y)$	$f_{323}(y)$	$f_{331}(y)$	$f_{332}(y)$	$f_{333}(y)$	$\Phi(\mathcal{C})$	Remark
1	1	1	1	1	$w^4 1$	1	1	1	1	1	$w^7 1$	$[108, 104, 3]$	BKLC
1	1	1	1	1	$w^8 1$	1	1	1	1	1	$w^4 1$	$[108, 104, 3]$	

****